

**WHAT IS CLAIMED IS:**

1. A method for performing authorization of an ignition key by using an engine control unit (ECU) and an ignition key that stores a key ID, a lock password and a key password, the method comprising the steps of:

5 (1) the ECU receiving the key ID from the ignition key and determining if the key ID is a registered ID;

10 (2) generating, if the key ID is the registered ID, a random number and encoding a stored lock password using the random number, and transmitting the random number and the encoded lock password to a transponder of the ignition key;

(3) the transponder decoding the lock password using the received random number and encoded lock password, then determining if the decoded lock password is identical to a stored lock password;

15 (4) the transponder encoding a key password using a stored key password, and transmitting the encoded key password to the ECU;

(5) the ECU decoding the received encoded key password, then determining if the decoded key password is identical to the stored key password; and

20 (6) releasing an ignition lock state if the decoded key password is identical to the stored key password.

2. The method of claim 1 wherein the ECU includes shift registers T and S, and the encoding of the lock password in step (2) comprises the steps of:

(7) initializing and modulating the shift registers T and S using the random number;

(8) generating a first session key; and

(9) encoding the stored lock password using the first session key, and

5 wherein the decoding of the lock password using the random number and encoded lock password in step (3) are performed using the same processes involved in encoding the stored lock password using the random number of step (2).

10 3. The method of claim 2 wherein the initialization of the shift registers of step (7) includes the step of generating a random number, and

15 wherein the shift register modulation of step (7) is realized by designating a plurality of functions that receive input of a plurality of bit values and calculate a single bit value; designating an F2 function that receives input of calculation result values from the functions and calculates bit values; and repeating processes in which the shift registers T and S are shifted to the left, and determining an LSB of the shift register S using the F2 function values and the random number.

20 4. The method of claim 3 wherein in the generation of the first session key of step (8), a plurality of functions are designated that receive input of a plurality of bit values and calculate a single bit value, an F3 function is designated that receives input of calculation result values from the functions and calculates bit values, and bits of the first session key are calculated from the F3 function values.

5. The method of claim 4 wherein the plurality of functions is identical to the plurality of functions of step (7), and the F3 function is identical to the F2 function.

6. The method of claim 1 wherein the ECU includes shift registers T and S,

wherein encoding of the stored key password of step (4) comprises the steps of:

(10) generating a second session key; and

(11) encoding the stored key password using the second session key,

and wherein the decoding of the encoded key password in step (5) is performed using the same processes as are involved in the encoding of the key password.

7. The method of claim 6 wherein in the generation of the second session key of step (10), a plurality of functions are designated that receive input of a plurality of bit values and calculate a single bit value, an F4 function is designated that receives input of calculation result values from the functions and calculates bit values, and bits of the second session key are calculated from the F4 function values.